

Gaps between equations and experiments in quantum cryptography

John M. Myers

Gordon McKay Laboratory, Division of Engineering and Applied Sciences,
Harvard University, Cambridge, MA 02138

and

F. Hadi Madjid

82 Powers Road, Concord, MA 01742

Abstract.

Traditional methods of cryptographic key distribution rest on judgments about an attacker. With the advent of quantum key distribution (QKD) came proofs of security for the mathematical models that define the protocols BB84 and B92; however, applying such proofs to actual transmitting and receiving devices has been questioned.

Proofs of QKD security are propositions about models written in the mathematical language of quantum mechanics, and the issue is the linking of such models to actual devices in an experiment on security. To explore this issue, we adapt Wittgenstein's method of *language games* to view quantum language in its application to experimental activity involving transmitting and receiving devices.

We sketch concepts with which to think about models in relation to experiments, without assuming the experiments accord with any model; included is a concept of one quantum-mechanical model *enveloping* another. For any model that agrees with given experimental results and implies the security of a key, there is an enveloping model that agrees with the same results while denying that security. As a result there is a gap between equations and the behavior recorded from devices in an experiment, a gap bridged only by resort to something beyond the reach of logic and measured data, well named by the word *guesswork*.

While this recognition of guesswork encourages eavesdropping, a related recognition of guesswork in the design of feedback loops can help a transmitter and receiver to reduce their vulnerability to eavesdropping.

1. Introduction

In a laboratory that has equations on a blackboard and devices[†] on a bench, a fair question is how do the equations and the devices connect? The terms of the equations act as words of a language used in the laboratory. People say or write these terms along with non-mathematical words (*e.g.* ‘screwdriver’) while they work with devices, an activity Wittgenstein characterized as a *language game* [1, 2, 3, 4]. Recently we brought the writing of equations and the using of devices into a common language game. This allowed us to prove that deciding to describe a particular laboratory situation by a particular quantum mechanical model takes something beyond logic and measured data, something aptly called a *guess* [5].

Here are three examples of questions in quantum cryptography resolvable only by augmenting equations and data by guesswork:

1. Alice and Bob interpret some equations as describing a transmitter and a receiver for quantum-cryptographic key distribution. How do they make or buy devices that behave in accord with those equations?

2. Bob uses quantum-electrodynamics to define photons in terms of creation operators, and Bob’s photodiode detector feeds current blips into an audio amplifier so he hears and counts them. Under what circumstances does counting blips give him a claim to say he counts photons?

3. Alice and Bob experiment with a transmitter and a receiver linked by an optical fiber, and their results agree with the predictions of a model in which it is proved they are secure against undetected eavesdropping using individual attacks. What use can they make of that proof?

We will show that quantum states are by no means ‘plainly visible’ in the devices of

[†] We think of ‘devices’ as being designed using quantum mechanics to serve practical purposes, and of ‘instruments’ as being used to test models in quantum mechanics. Often the same piece of gear can play either role, and we shall use the word ‘device’ to mean either.

experiments on quantum cryptography; rather there is a gap, as pictured in figure 1, between states as terms in equations and results recorded from devices on a laboratory bench. To show this gap and its bridging by guesswork, we will sketch a conceptual framework in section 2, and then turn in section 3 to quantum cryptographic key distribution as an appealing arena for examples. Cryptographers know that relying on a theory does not bind one's enemy to rely on the same theory. They know too that abstractions endemic to theories are likely targets for cryptographic attack, so they can well imagine that a proof of the security of quantum key distribution might not be the last word [6]. By seeing gaps in physics where logic cannot reach and guesses are indispensable, we will see both limitations to proofs of the security of quantum key distribution and opportunities to improve security.

2. Concepts for bridging equations and experiments

Preliminary to showing how guesses bridge the gap between equations and experiments, we introduce the concept of a quantum mechanical model of an experimental trial; we also attend to *trial-to-trial management* and introduce the *envelopment of one model by another* as a building block for sections 3 and 4.

2.1. Models of experimental trials

Quantum mechanics provides language in which to write equations for various probabilities and to relate these equations logically to one another. Proofs of QKD security apply equations for probabilities as models of devices expected to be used to communicate keys. Quantum mechanical operators and state vectors are germane to QKD security only as they appear as components in equations that define probabilities in models that someone applies to actual or anticipated devices.

To test a model of QKD one subjects the devices to a run of experimental trials, each

of which involves setting up devices and recording results. In order that trials of devices can test a model, the model must speak of the devices, and for this the operators and state vectors must somehow be linked to these devices.

Appreciating the need to link state vectors to devices requires you to resist a temptation. In planning a test of a model that involves quantum states, avoid picturing yourself ‘in a Hilbert space of these states,’ an intangible world disconnected from the world of prisms and fibers on a bench. Instead, look at how you can use quantum states in calculations. Momentarily set aside the picture of state vectors as denizens of a Hilbert-space world, and notice how you write characters for quantum states into a computer memory, preferably the memory of the same computer that manages the devices during a run of experimental trials. This puts your writing of quantum states and calculating with them into a common world with the handling of prisms and fibers.

That still leaves the problem of how to attach state vectors and operators, as terms in equations of a model, to devices in a laboratory. One goes half way by deciding to attach states and operators as terms in equations to various settings of the knobs and levers by which the devices are configured in a trial, to get state-valued functions and operator-valued functions of the knob and lever settings [5]. To complete the attachment, one has to decide which device settings go with which states and operators. Once accomplished, the attachment of the states and operators to device settings converts the usual quantum mechanical probabilities of outcomes for given states and operators to probabilities of outcomes for given device settings. With this trick one gets equations interpreted as asserting something about devices. The first kind of model to consider can be called a quantum-mechanical model of devices or, for short, QM-model. Later we will use models of this type as a foundation on which to build some other kinds of models.

A QM-model α consists of a triple of functions that, in combination, generate probabilities of outcomes for various set-ups of devices. Simplifying the full description given

in appendix A, one can view these functions as follows. (1) State preparation is expressed by a function $|\text{state}_\alpha(\text{set-up})\rangle$ from the domain of set-ups of devices to state vectors; (2) evolution over a time duration is expressed by a function $U_\alpha(\text{set-up})$ from the domain of set-ups of devices to unitary operators; and (3) a measurement process that generates results is expressed by a function from set-ups of devices to operators, most generally in the form of a positive operator-valued measure (POVM) as a set of detection operators, one for each possible outcome, $M_{\alpha,\text{outcome}}(\text{set-up})$ [7]. This triple of functions generates probabilities of outcomes as a function of set-up, asserted by model α , according to the usual rule:

$$\begin{aligned} & \Pr_\alpha(\text{outcome}|\text{set-up}) \\ &= \langle \text{state}_\alpha(\text{set-up}) | U_\alpha(\text{set-up}) M_{\alpha,\text{outcome}}(\text{set-up}) U_\alpha^\dagger(\text{set-up}) | \text{state}_\alpha(\text{set-up}) \rangle, \end{aligned} \tag{1}$$

where the subscripts α indicate that the functions to which they are attached are particular to model α so another model would involve other functions.

Analyzing the receipt of a cryptographic key from the standpoint of quantum mechanics, one is interested in the question the other way around. Given an outcome, Bob (or Eve) wants to know what state Alice transmitted, a subject addressed by quantum decision theory via Bayes rule [7, 8].

2.2. Computer management of trials and models

In order to describe the set-up of devices sufficiently to prove the need for guesswork in choosing a model for QKD, we restrict ourselves to describing only a part of setting up that can be controlled by a Classical digital Process-control Computer (CPC). This part is described by the commands transmitted from the CPC to actuators internal to these devices. Such commands call, for example, for a stepping motor to rotate a polarizer to a certain angle. The same CPC serves to record the writing of QM-models in which set-ups are expressed

as CPC-commands and to execute quantum-mechanical calculations involving these models. (The proof of Proposition 1 in section 3 assumes only that some choices of set-up can be CPC mediated, not that everything in setting up an experiment is CPC mediated.) As pictured in figure 2, the CPC:

(1) provides an investigator with a display by which to experience results of trials reported by the devices to the computer;

(2) gives the investigator a keyboard by which to operate the computer;

(3) makes a record of what the investigator does (such as entering equations into programs that, when executed, control the devices); and

(4) (in various ways) allows feedback from the devices to modify the equations [5].

Section 3 presents examples in which devices are controlled jointly by Alice, Bob, and Eve, each via a CPC; in this case a ‘command’ is taken to be the concatenation of commands from the three CPCs of Alice, Bob, and Eve, respectively.

2.3. Envelopment of one QM-model by another

In testing a QM-model against results of experimental trials, one tests the probability distribution calculated from the model against relative frequencies extracted from measured results.[‡] Any such test of the probability distribution tests the triple of functions that define the model, but only in the combination of equation (1); one cannot test any of the functions separately without assuming the others. In particular, one cannot test quantum states independently of the other two functions.[§] When the probabilities of a model α are found to closely match relative frequencies of outcomes for the various settings used in a run

[‡] As discussed in [5], that extraction itself requires guesswork.

[§] Claims that quantum tomography allows a scientist to determine a state experimentally [9, 10] assume that the scientist knows the operators that describe the measuring instrument. But how does the scientist determine these operators? By using the instruments to ‘measure known states’: without guesswork, the scientist is stuck in a circle, as an example to come will show.

of experimental trials of devices, one can still ask what other models agree as well with the same relative frequencies.

To sharpen this question we define the first of two relations among QM-models. By restricting the set of commands of a QM-model to a subset, one generates what can be called a restriction of the QM-model. When an experiment confirms a QM-model, it actually confirms, at most, the restriction of the QM-model to commands tested, and often these are a small subset of the commands of the model. Suppose model α is such a restriction, and that it generates probabilities that closely match the relative frequencies of a run of trials. Then any model β agrees with the experimental trials if and only if it agrees with this model α . Hence we want to know: what models other than model α predict the same probabilities as does α concerning the settings covered by C_α ? (Notice that this question is made possible by the attachment of states and operators to settings of devices.) As we shall see, for any QM-model α a large set of other QM-models, defined by a variety of triples of functions, produce the same probabilities for settings of C_α . As a result, a tight screening of probability distributions by experiments induces only a loose screening of state- and operator-valued functions. This looseness in the testability of quantum states limits the role of proofs in quantum cryptography.

To clarify this looseness we introduce the concept of an *envelopment* of one model by another. Let O_α be the set of outcomes for model α . Given two QM-models α and β , suppose there is a function f from a subset of $C_\beta \times O_\beta$ to $C_\alpha \times O_\alpha$, with the property of preserving probabilities in the sense that:

$$(\forall b \in C_\alpha, j \in O_\alpha) \Pr_\alpha(j|b) = \sum_{(b',j') \in f^{-1}(b,j)} \Pr_\beta(j'|b'). \quad (2)$$

We say such a function f *envelops* α by β . An enveloping model β need not preserve inner products of quantum states of model α , and for this reason the inner products of quantum states cannot be determined from experimental results without augmentation by guesswork.

In the case to be discussed in section 3, there is no ‘mixing’ by the mapping f , which is to say there exist functions g and h such that $f(b, j) = (g(b), h(j))$, and the envelopment of model α by model β exhibits the provocative inequality:

$$|\langle \psi_\beta(b) | \psi_\beta(b') \rangle| \ll |\langle \psi_\alpha(g(b)) | \psi_\alpha(g(b')) \rangle|, \quad (3)$$

with implications for security shortly to be developed.

3. Application to quantum cryptography

For quantum key distribution using the protocols BB84 [11] or B92 [12], published arguments for the security of the key [11, 12, 13, 14, 15, 16, 17] assume a QM-model α (augmented by Bayes rule), according to which, at each trial, Alice’s transmitter receives a command b_A from some finite set of possible commands and ‘prepares a unit state vector’ $|\psi_\alpha(b_A)\rangle$. In both early work that ignores noise and in later work that accounts for noise (and invokes privacy amplification [15, 16, 18]), claims of security assume that inner products of the ‘unit state vectors’ that Alice can transmit are experimentally verifiable without regard to what devices Eve might invent. The argument is that, given suitable magnitudes of inner products $S_\alpha(b_A, b'_A) \equiv |\langle \psi_\alpha(b_A) | \psi_\alpha(b'_A) \rangle|$, any snooping by Eve disturbs Alice’s states in ways Alice and Bob can almost surely detect as an increase in the error rate in Bob’s reception or the rate of inconclusive outcomes [19] or both (when they compare notes publicly, at the sacrifice of some of the bits of the key).

To what extent can experimental results on devices confirm a model α that, based on inner products, asserts security of QKD? Alice and Bob need to be secure not just against an attack by snooping devices that they use when they play Eve’s part in Red-Blue exercises, but against all of the attacks, within some class, that a real Eve might invent. Are Alice’s inner products verifiably independent of Eve’s inventions?

To claim experimental confirmation of the security implied by inner products of model

α is to claim that

- a) the probabilities calculated from model α match closely the relative frequencies of experimental results, and
- b) no other QM-model (say one with smaller inner products) that challenges that security produces the same probabilities that match those relative frequencies.

Although attachments of models of quantum cryptography to actual devices have been questioned [15, 20], the possibility of enveloping a model α by a model β having smaller inner products went unnoticed, with the consequence that the need to make the claim (b)—no model with smaller inner products fits the experimental results—also went unnoticed.

The published arguments for security assume “any attack that Eve might invent” is equivalent to “any QM-model that Eve might implement that has the inner products of model α ”. Thus the experimental confirmation of security depends on the notion that inner products are experimentally testable. The trouble is that, as shown in section 2, experiments cannot test states and their inner products *per se* but only the probabilities they generate. For example, suppose a run of experimental trials shows a close match to the probabilities of a QM-model α that speaks of certain inner products $S_\alpha(b_A, b'_A)$. Do these trials ‘demonstrate (*e.g.* single-photon) states’ having these inner products? The answer is “*no*,” because for any model α there is always an envelopment by an alternative model β that produces probabilities in agreement with α concerning the experimental results that Alice and Bob have on hand, but generates these probabilities on the basis of different states with smaller inner products. Because of its smaller inner products, the model β points to something outside of model α that, if Eve can do it, allows her to eavesdrop undetected.

3.1. Example of conflicting models that fit the same measured data

Among widely used models of the security of quantum key distribution against undetected individual attacks, there are two cases to consider, corresponding to Eve measuring Alice's signal directly, or, using a probe, indirectly. Deferring models of Eve's use of a probe to appendix B, we consider an individual eavesdropping attack in which Eve measures Alice's signal and tries to transmit a signal to Bob, aiming to match what would have come from Alice. Any model α asserting security against this attack rests on an inner product for Alice's possible states. We now show how to envelop model α by a model β having a smaller inner product but producing the same probabilities as model α .

The model α assumes that the command set C_α consists of concatenations of a command b_A from Alice to determine a state vector and a command b_E from Eve to select a POVM. These commands produce Alice's state vector $|v_\alpha(b_A)\rangle \in \mathcal{H}_\alpha$, and Eve's measurement expressed by a POVM $M_\alpha(b_E)$ which has a detection operator $M_\alpha(b_E; j_E)$ acting on \mathcal{H}_α , associated with outcome j_E . Model α implies that the conditional probability of Eve obtaining the outcome j_E given her command b_E and Alice's command b_A is

$$\Pr_\alpha(j_E|b_A, b_E) = \langle v_\alpha(b_A) | M_\alpha(b_E; j_E) | v_\alpha(b_A) \rangle, \quad (4)$$

implying that the error rate for Eve in distinguishing among Alice's commands, asserted by model α , depends on the inner products $S_\alpha(b_A|b'_A)$.

Proposition 1 *Given any such model α with inner products $S_\alpha(b_A, b'_A)$ and given any $0 \leq r < 1$, there is a model β that gives the same conditional probabilities of Eve's outcomes for all her commands belonging to E_α , so that*

$$(\forall b_A \in A_\alpha, b_E \in E_\alpha) \Pr_\beta(j_E|b_A, b_E) = \Pr_\alpha(j_E|b_A, b_E) \quad (5)$$

while

$$S_\beta(b_A, b'_A) \leq r S_\alpha(b_A, b'_A). \quad (6)$$

Proof: Motivated by the idea that, unknown to Alice, her transmitter signal might generate an additional “leakage” into an unintended spurious channel that Eve reads, we construct the following enveloping model β which assumes:

- (i) the same set of commands for Alice,
- (ii) a larger Hilbert space $\mathcal{H}_\beta = \mathcal{H}_{\text{leak}} \otimes \mathcal{H}_\alpha$ in which Alice produces vectors $|v_\beta(b_A)\rangle = |w_\beta(b_A)\rangle \otimes |v_\alpha(b_A)\rangle$, with $|w_\beta(b_A)\rangle \in \mathcal{H}_{\text{leak}}$;
- (iii) a larger set of commands for Eve, $E_\beta = E_\alpha \sqcup E_{\text{extra}}$ (disjoint union);
- (iv) a POVM-valued function of Eve’s commands to her measuring instruments, with detection operators

$$M_\beta(b_E; j_E) = \begin{cases} \mathbf{1}_{\text{leak}} \otimes M_\alpha(b_E; j_E) & \text{for all } b_E \in E_\alpha, \\ \text{Eve's choice of POVM to distinguish} & \\ |v_\beta(0)\rangle \text{ from } |v_\beta(1)\rangle & \text{if } b_E \in E_{\text{extra}}. \end{cases} \quad (7)$$

According to model β , if Eve chooses any measurement command of E_α , equation (4) holds. But model β speaks not of the vectors $|v_\alpha(b_A)\rangle$ but of other vectors having an inner product of magnitude

$$\begin{aligned} S_\beta(b_A, b'_A) &\stackrel{\text{def}}{=} |\langle v_\beta(b_A) | v_\beta(b'_A) \rangle| \\ &= |\langle w(b_A) | w(b'_A) \rangle| |\langle v_\alpha(b_A) | v_\alpha(b'_A) \rangle|. \end{aligned} \quad (8)$$

We can choose the unit vectors $|w(b_A)\rangle$ at will; in particular nothing excludes choosing them so that $\forall b_A \neq b'_A, |\langle w(b_A) | w(b'_A) \rangle| \leq r$, from which the proposition follows. \square

3.2. Impossibility of positive tests of inner products

Models of the form of model β with its $r < 1$ thus match any data that match model α while denying security of the key. Given the two QM-models, α and β , that disagree about cryptographic security while agreeing about probabilities for commands of C_α , one would like to decide between the conflicting models by an experiment. But, without guesswork, this

is impossible, for the enveloping model β is no description of instruments on hand; instead, it is a picture of behavior that Eve might try to achieve by inventing a snooping device not yet known. Nor does model β (nor any QM-model) say of itself how to implement it, because it speaks only of states and operators rather than of the prisms and optical fibers that one can find in a supply room. Implementing model β would require invention and discovery, such as gaining access to a channel carrying leakage states [21, 22]. For this reason there can be no positive experimental test of the inner products of quantum states, nor of claims of cryptographic security based on such inner products. Indeed, to claim security against ‘all the eavesdropping devices that Eve might invent’ for individual attacks is to misuse the word ‘all’; by confusing ‘all devices’ described by a model α with ‘all the models’ consistent with experiments that accord with probabilities expressed by model α . It is for this reason that the application of a model to actual devices takes guesswork. The notion that experiments can determine Alice’s inner products independent of Eve’s inventions is faulty, because it confuses experimental validation of probabilities, which is possible, with experimental validation of inner products of quantum states, which, as we have shown, is impossible to disentangle from guesswork.

In more practical terms, to experimentally confirm QKD security by ‘seeing a single-photon state,’ one must see the absence of correlated signals that accompany it, which Eve might receive, and nothing in Alice and Bob’s modeling and experiments can exclude a real Eve from finding such a signal in a place Alice and Bob never thought to look, such as light emitted by Alice’s transmitter in a spurious frequency band [15].

4. Quantum physics between trials: a glimpse of feedback

It is often advantageous to introduce feedback into a run of trials, using the outcome of one trial in setting up a next trial, as illustrated in figure 3 [23, 24, 25, 26, 27, 28, 29, 30, 31].|| By studying trial-to-trial adjustment brought about by feedback loops designed using QM-models, we will win fresh insight into the bridging of equations and devices of experimental trials. The typographical view of equation writing introduced in section 2, with CPCs as equation holders, allows one to view a feedback loop as a special sort of device, a device containing an equation-holding CPC which a scientist uses to link equations of QM-models (and other equations) to operations of other devices. This picture opens up a place in theoretical physics in which to investigate trial-to-trial adjustment.

To define a feedback loop, a designer specifies a *control function* that maps results of completed trials and other records on hand to actions to be taken in response to these. The specification of the control function can make use of QM-models. But neither a QM-model nor a Schrödinger equation expresses a place in which an outcome from one trial can enter to influence a state preparation at a subsequent trial; on the contrary, trial-to-trial adjustments of devices take place in a space outside of QM-models, so to speak. To deal with feedback in a quantum context, one has to implant QM-models as components of larger models, which we call *control models*, which contain control functions that express how a CPC responds to outcomes. Its need for feedback cements quantum physics into a classical environment of CPCs that command the devices and record the results.

4.1. Comparisons of theory and experiment, in the presence of feedback

In a feedback situation, CPCs that accompany other devices or are embedded in them are part of the experimental instrumentation, and so are their files housing the equations that define

|| We do not discuss ‘coherent quantum feedback’ in the sense of ref. [32]

a control function. These files of equations are used not for analysis but to define actions of devices, which puts an end to any categorical distinction between equations and devices. This poses a question of just what one compares with what in an experimental trial, for one cannot, in this situation, compare an ‘equation as something unphysical’ against ‘behavior of physical devices free of equations’. One does, however, compare predictions calculated from a QM-model and other equations of a control model with experimental trials in which the same equations take part in programs of CPCs that control the devices. *I.e.*, one compares a ‘use of equations and guesses to make a prediction’ against ‘behavior of devices controlled by CPCs programmed using the same equations’ (and possibly other equations as well).

4.2. Timing in quantum cryptography

Quantum cryptography provides an arena for examples of trial-to-trial adjustments, pertaining to timing. In quantum key distribution, Bob’s receiver is intended to detect a sequence of signals transmitted by Alice. Bob’s receiver (as well as Eve’s snooping devices) depends on keeping in step with the signals of the sequence transmitted by Alice. Besides the need to correlate detections with Alice’s acts of transmission, there can be a need to gate a receiver off except in a narrow time interval around the arrival of each signal.

Keeping the receiver in step with the signals arriving from the transmitter requires one or another use of results of one trial to regulate the receiver timing for another trial. That is synchronization, an important form of trial-to-trial adjustment. For understanding synchronization, it is necessary to look for a quantum description of reception that describes a receiver only imperfectly timed. This leads us to the notion of a receiver that measures, or at least estimates, the time difference between the arrival of a signal and the gating of its detector, a time difference we call *skew*. For a quantum-mechanical model to express this additional distinction of temporal skew in detection, it has to allow for a larger variety of quantum states than did models α and β above, with the skew as an additional argument,

which entails expanding the dimension of the Hilbert space beyond that of model α .

To glimpse an expanded model γ that envelops the model α of section 3, and that allows a designer to picture timing, suppose a receiver is designed to expect the k -th signal at reading t_k of its clock, and that the clock is fast by a *skew* s_k ; then the signal arrives not at clock reading t_k but in a small interval around $t_k - s_k$. To allow for skew, model γ must have a Hilbert space \mathcal{H}_γ , of dimension higher than that of \mathcal{H}_α (if that is finite), along with states $|v_\gamma(b_A, s_k)\rangle$ that are functions not only of Alice's commands in $A_\gamma = A_\alpha$, but also of the skew s_k of Bob's clock. We conclude that for model α to accord with the behavior of an imperfectly synchronized receiver, there must be an envelopment f of model α by such a model γ with the property that:

$$(\forall -s_0 < s_k < s_0) f(|v_\gamma(b_A, s_k)\rangle) = |v_\alpha(b_A)\rangle. \quad (9)$$

An interesting topic for future work is the elaboration of models such as γ and their application to more subtle forms of synchronization, with which Alice and Bob can advance their cause by making it more difficult for Eve to make guesses necessary to eavesdropping. For example if Alice and Bob manage to synchronize of Bob's receiver while Alice transmits using a deliberately irregular clock rate, Eve has a problem determining when to gate her snooping receiver.

5. Discussion

To base QKD security only on proofs is to forget the crucial point that proofs are purely mathematical. A proof of a proposition asserting security shows that the proposition, written as an equation, follows from assumptions by logic, without guesswork. Prominent in the assumptions are inner products. In simple and rough terms, a proof of QKD security shows that if Alice's transmitter is modeled by a certain inner product between two possible states, then the model says: 'any individual eavesdropping attack is detectable.' But do we buy the

assumption on which the conclusion of the model rests? Can one decide this by applying logic to experimental tests of the model? More precisely, suppose relative frequencies of outcomes obtained in a run of experimental trials agree with the probabilities calculated from the inner products assumed in the model: do we then buy the model?

We have tried to avoid garbling logical connections within mathematics, on one hand, with the application of that mathematics to actual devices on the other. By analyzing not just a single model but a multiplicity of models (all purely mathematical) we made plain a security issue: for any experimental data on hand, more than one model can fit them perfectly, and among the models that fit the data are models with widely differing inner products. Thus choosing one of these models while rejecting others requires reaching outside the measured data and the logic of models, as asserted by our Proposition 1. Because inner products, central to QKD security, vary widely over those models that exactly fit the measured data, the measured data cannot determine the value of the inner product. Therefore the inner product is not measurable, and assuming that any model, with its inner products, applies to particular devices reaches beyond logic into the realm of guesswork.

Like any proof, our proof of Proposition 1 clarifies the effect of rules of logic. This proof escapes the question “are we sensible to apply it to cryptography” because we do not apply it to devices *per se*, but use it only to elucidate the logic of *arguments* about cryptography, arguments that, as it turns out, overlook choices of model that are apparent once the model that asserts security has been set in the context of a language game in which it competes with other models.

The world of cryptography, as we have described it, is a multi-model world in which each side must guess to choose models that guide actions. By recognizing feedback, as in section 4, we show choices of models, with their guesswork, that enter responses to experimental results, and hence enter the use of outcomes to manage experiments. Records in the memory of a computer used in a feedback loop can reflect guesses within a structure of equations and

devices. By introducing CPCs, with their capacity to mediate between a scientist and devices and to record guesses as choices of models used in device-controlling programs, we make a beginning toward exploring the structure of guesswork in the bridging of equations to devices.

Acknowledgments. We thank Howard E. Brandt for reading an early draft and giving us an astute critique, indispensable to this paper. We thank John Lowry, Donald Nicholson, Bahaa Saleh, Alexander Sergienko, Malvin Teich, and Tai T. Wu for contributing substantially to this paper. This work was supported in part by the Air force Research Laboratory and DARPA under Contract F30602-01-C-0170 with BBN Technologies.

Appendix A. Formal definition of QM-models and their envelopment

To formally present *QM-models* and the enveloping of one by another, it is convenient to introduce a category having structures of equations of QM-models as its objects [33]. We abuse language by calling these structures QM-models. Any QM-model α consists of: a domain C_α of commands from CPCs (which we interpret as commands that set up devices), a set of possible outcomes O_α , a Hilbert space \mathcal{H}_α , and a triple of functions, namely (1) $|\psi_\alpha\rangle : C_\alpha \times O_\alpha \rightarrow \mathcal{H}_\alpha$, (2) $U_\alpha : C_\alpha \times O_\alpha \rightarrow \{\text{unitary operators on } \mathcal{H}_\alpha\}$, and (3) $M_\alpha : C_\alpha \times O_\alpha \rightarrow \{\text{semipositive hermitian operators on } \mathcal{H}_\alpha\}$, subject to the constraint that makes M_α work as a positive-operator-valued measure (POVM), namely that

$$(\forall b \in C_\alpha) \sum_{j \in O_\alpha} M(b; j) = \mathbf{1}, \quad (\text{A.1})$$

where the $\mathbf{1}$ denotes the identity operator on \mathcal{H}_α . The triple of functions defines a probability distribution on outcomes given the set-up $b \in C_\alpha$ by the rule

$$\text{Pr}_\alpha(j|b) = \langle \psi_\alpha(b; j) | U_\alpha^\dagger(b; j) M_\alpha(b; j) U_\alpha(b; j) | \psi_\alpha(b; j) \rangle. \quad (\text{A.2})$$

In the examples in the paper, the state preparation expressed by $|\psi_\alpha\rangle$ depends only on a command and not on an outcome, as does the unitary transform U_α ; in that case equation

(A.1) becomes

$$\Pr_\alpha(j|b) = \langle \psi_\alpha(b) | U_\alpha^\dagger(b) M_\alpha(b; j) U_\alpha(b) | \psi_\alpha(b) \rangle. \quad (\text{A.3})$$

We remark that if the devices are controlled by more than one CPC, as is the case in cryptographic examples, then the command b that specifies a set-up of devices is a composite of commands from the various CPCs. For example if the set-up is established by the three CPCs of Alice, Bob, and Eve, respectively, a command b has the form $b = b_A \parallel b_B \parallel b_E$ where \parallel denotes concatenation of the commands from the three parties.

The single set $C_\alpha \times O_\alpha$, which expresses the possibilities of set-ups of devices for a run of trials along with the possible outcomes, is the domain for all three functions that represent state preparation, evolution, and measurement. Sometimes one wants to suppose that one device prepares a state, another device is responsible for evolution, and a third measures. By adding assumptions beyond those by which we defined a QM-model, one can generate a specialization of a QM-model that expresses such a notion, as if the function $|\psi_\alpha\rangle$ had a domain distinct from that of U_α and M_α . For example, one can specialize a QM-model so that the state $|\psi_\alpha(b, j)\rangle$ depends only on b_A and not on the commands b_B and b_E (concatenated with it to form $b \in C_\alpha$), nor on the outcome j in O_α . A function $|\psi'_\alpha(b_A)\rangle$ can always be written as a function $|\psi_\alpha\rangle$ on $C_\alpha \times O_\alpha$ for which variation of the argument j in O_α makes no change in the value of the function, and similarly, variation in the b_E and b_B parts of b make no change; for this reason, we can (and do) look at a function $|\psi'_\alpha(b_E)\rangle$ of one variable as a special case of the function $|\psi_\alpha(b, j)\rangle$ of two variables. A reason to formulate all three functions with the more general domain $C_\alpha \times O_\alpha$ is that, as discussed in [5], the supposition that one device prepares a state independent of other devices is unprovable; it is introducible only as an additional assumption. In addition, including the O_α factor in the domain of $|\psi\rangle$ allows the modeling of randomness in state preparation.

Given two models α and β of the category, a *morphism* from β to α is defined by a function f from a subset (not necessarily proper) of $C_\beta \times O_\beta$ to $C_\alpha \times O_\alpha$, with the property of preserving probabilities in the sense that:

$$(\forall b \in C_\alpha, j \in O_\alpha) \Pr_\alpha(j|b) = \sum_{(b', j') \in f^{-1}(b, j)} \Pr_\beta(j'|b'). \quad (\text{A.4})$$

Given such a morphism, QM-model β will be said to *envelop* QM-model α , and the morphism will be called an *envelopment*. When the morphism f is such that there are command-outcome pairs in $C_\beta \times O_\beta$ having positive probabilities but no image under f in $C_\alpha \times O_\alpha$, model α is a special case of model β with respect to the probabilities it predicts (but not necessarily with respect to its internal structure of inner products).

In some cases, an envelopment f from a model β to a given model α preserves inner products in the sense that $|\langle \psi_\alpha(f(b; j)) | \psi_\alpha(f(b'; j')) \rangle| = |\langle \psi_\beta(b; j) | \psi_\beta(b'; j') \rangle|$. For most of the envelopments, however, this is not the case. It is a mistake in logic to confuse the property of envelopment with the special case of envelopment that preserves inner products.

An application of envelopment is the finding, demonstrated in section 3, that a model β can envelop a model α *without* preserving inner products. In the case discussed in that section, there is no ‘mixing’ by f , which is to say there exist functions g and h such that $f(b, j) = (g(b), h(j))$, and the envelopment of model α by model β exhibits the provocative inequality:

$$|\langle \psi_\beta(b) | \psi_\beta(b') \rangle| \neq |\langle \psi_\alpha(g(b)) | \psi_\alpha(g(b')) \rangle|, \quad (\text{A.5})$$

which allows for security expressed by a model α to be contradicted by an enveloping model β .

Appendix B. Security models involving a probe and a defense function

Arguments for the security of quantum key distribution that deal with noisy channels call for privacy amplification to distill a secure key [18]. These arguments center on a *defense function*

[15, 16, 19, 34]. Defense functions have been analyzed for models embellished to speak of Eve's use of a probe [14]. In such a model α , Alice chooses one of several state vectors in one Hilbert space $\mathcal{H}_{\text{sig},\alpha}$ while Eve generates a fixed vector in a different Hilbert space $\mathcal{H}_{\text{probe},\alpha}$, and the tensor product of Alice's choice of state vector and Eve's fixed probe vector evolves unitarily in an interaction, after which Eve and Bob make measurements, Eve confined to the probe sector and Bob to the signal sector.

To see the consequence of signal leakage for defense functions and probes, suppose that Alice and Bob use model α which assumes that Alice chooses between state vectors $|v_\alpha(0)\rangle$ and $|v_\alpha(1)\rangle$ with inner product having a magnitude $S_\alpha = |\langle v_\alpha(1)|v_\alpha(0)\rangle|$. Assuming model α , Alice and Bob determine a defense function $t(n, e_T)$, as discussed in [16]; in order to mark its dependence on model α and especially its dependence on the inner product of S_α , we write this as $t_\alpha(n, e_T, S_\alpha)$. As in the simpler case of section 3, if the inner products for distinct signal vectors are all zero, Eve can learn everything without causing any effect that Alice and Bob can detect; and, as before, Alice's state vectors are model-dependent, and so are their inner products. For this reason, it is easy to adapt the reasoning of Proposition 1 to prove:

Proposition 2 *If a model α asserts that Alice and Bob can distill a key that is secure against measurements commanded by Eve from a set of commands E_α , then there exists another model β that matches the predictions of model α for the commands in E_α but, by virtue of different inner products, makes additional commands available to Eve that make the key insecure.*

- [1] Wittgenstein L 1958 *Philosophical Investigations* 2nd edn (Oxford: Blackwell)
- [2] Wittgenstein L 1975 *Philosophical Remarks* (Oxford: Blackwell)
- [3] Wittgenstein L 1969 *Philosophische Grammatik* (Oxford: Blackwell)
- [4] Wittgenstein L 1974 *Bemerkungen über die Grundlagen der Mathematik* (Frankfurt: Surhkamp)
- [5] Myers J M and Madjid FH 2002 in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millenium* Contemporary Mathematics Series (Providence, RI: American Mathematical Society); also 2000 *e-print* quant-ph/0003144
- [6] Lowry J 2001 Private communication
- [7] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic)
- [8] Holevo A S 1982 *Probability and Statistical Aspects of Quantum Theory* (New York: North-Holland)
- [9] Raymer M G 1997 *Contemp. Phys.* **38** 343
- [10] Poyatos J F, Cirac J I and Zoller P 1997 *Phys. Rev. Lett.* **78** 390
- [11] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore)* (New York: IEEE) p 175
- [12] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
- [13] Ekert A K, Huttner B, Massimo Palma G and Peres A 1994 *Phys. Rev. A* **50** 1047
- [14] Fuchs C A and Peres A 1996 *Phys. Rev. A* **53** 2038
- [15] Slutsky B A, Rao R, Sun P-C and Fainman Y 1998 *Phys. Rev. A* **57** 2383
- [16] Slutsky B A, Rao R, Sun P-C, Tancevski L and Fainman S 1998 *Appl. Opt.* **37** 2869
- [17] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
- [18] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 *IEEE Trans. Info. Theory* **41** 1915
- [19] Brandt H E 2000 *Phys. Rev. A* **62** 042310
- [20] Lo H-K 1999 *e-print* quant-ph/9912011
- [21] Myers J M and Brandt H E 1997 *Meas. Sci. Technol.* **8** 1222
- [22] Huttner B, Muller A, Gautier J D, Zbinden H and Gisin N 1996 *Phys. Rev. A* **54** 3783
- [23] Jakeman E and Jefferson J H 1986 *Optica Acta* **33** 557
- [24] Wiseman H M and Milburn G J 1993 *Phys. Rev. Lett.* **70** 548
- [25] Madjid F H and Myers J M 1993 *Ann. Phys., NY* **221** 258
- [26] Haus H A and Yamamoto Y 1986 *Phys. Rev. A* **34** 270
- [27] Shapiro J H, Saplakoglu G, Ho S-T, Kumar P, Saleh B E A and Teich M C 1987 *J. Opt. Soc. Am. B* **4** 1604

- [28] Wiseman H M 1994 *Phys. Rev. A* **49** 2133
- [29] Doherty A C and Jacobs K 1999 *Phys. Rev. A* **60** 2700
- [30] Doherty A C, Habib S, Jacobs K, Mabuchi H and Tan S M 2000 *e-print* quant-ph/9912107
- [31] Doherty A C, Jacobs K and Jungman G 2000 *e-print* quant-ph/0006013
- [32] Lloyd S 2000 *Phys. Rev. A* **62** 022108
- [33] Lang S 1993 *Algebra* 3rd edn (Reading, MA: Addison-Wesley)
- [34] Brandt H E 1999 *Phys. Rev. A* **59** 2665

Figure Captions

Figure 1. Gap between analyzing with models and using devices

Figure 2. Models and devices reflected in files of CPC

Figure 3. CPC-controlled adjustment in response to outcomes

"Gap" between models and instruments

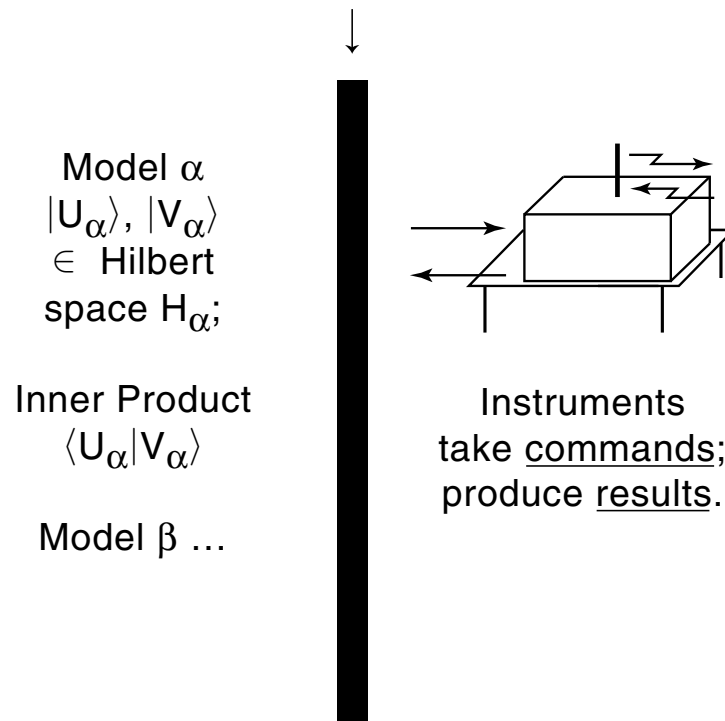


Figure 1. Gap between analyzing with models and using devices.

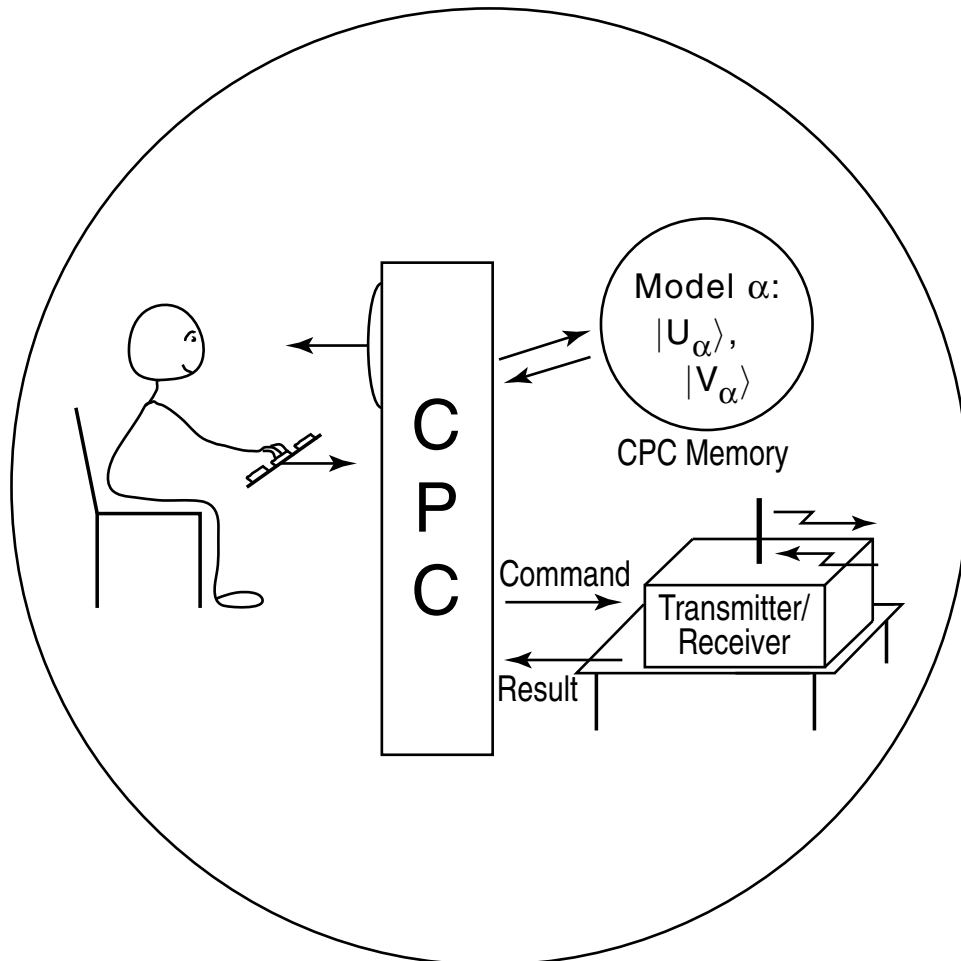


Figure 2. Models and devices reflected in files of CPC.

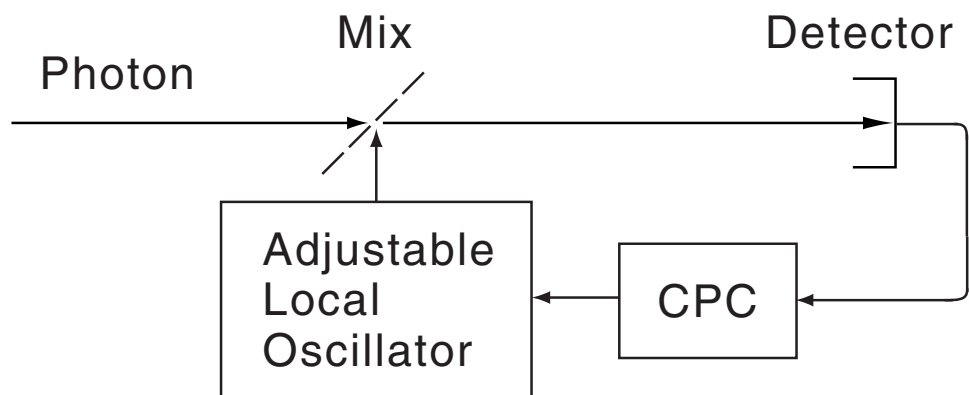


Figure 3. CPC-controlled adjustment in response to outcomes.